REMARKS

The Examiner has rejected Claims 1-3, 5-6, 8-22, 24-32 and 34-37 under 35 U.S.C. 103(a) as being unpatentable over Hodges (U.S. Patent No. 6,269,456) in view of Van Huben et al. (U.S. Patent No. 6,327,594). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has responded to applicant's arguments regarding applicant's claimed technique "whereby the central service computer and the user computer are each configured to send the new antivirus file to the other of the central service computer and the user computer to update the antivirus database" (see this or similar, but not identical, language in each of the foregoing claims). Specifically, the Examiner has stated that there are no claim limitations in the body of the claim that specifically require both the user computer and the central service computer to have antivirus databases. The Examiner has thus suggested an amendment requiring "both the user computer and the central service computer to have antivirus databases that are mutually updated by the method disclosed in Figure 6 of applicant's specification to help clarify this issue."

First, applicant respectfully points out applicant's claimed "comparing the antivirus databases of the central service computer and the user computer" which is clearly a claim limitation in the body of the claim that specifically requires both the user computer and the central service computer to have antivirus databases. Nevertheless, for further clarification, applicant respectfully asserts that an amendment, as suggested by the Examiner, has been made to each of the independent claims. Specifically, applicant has amended each of the independent claims to include the following highlighted claim language:

"whereby the central service computer and the user computer are each configured to send the new antivirus file to the other of the central service computer and the user computer to update the antivirus database such that the antivirus database of the central service computer is capable of being updated by the user computer and the antivirus database of the user computer is capable of being updated by the central service computer (see the same or similar, but not necessarily identical language in each of the independent claims).

In view of such clarification, applicant respectfully asserts that Hodges, as relied on by the Examiner, merely teaches antivirus update files that are received by a client computer, and a central antivirus server that is only generally kept up-to-date with antivirus files (see Col. 7, lines 45-63 and Col. 9, lines 53-55). Clearly, a general teaching of a central antivirus server that is kept up-to-date, as in Hodges, does not meet applicant's present claim language, namely that "the antivirus database of the central service computer is capable of being updated by the user computer and the antivirus database of the user computer is capable of being updated by the central service computer" (emphasis added).

Still with respect to each of the independent claims, the Examiner has failed to address applicant's arguments with respect to applicant's claimed technique "wherein the user computer is configured to send the new antivirus file to the central service computer to update the virus database, if is determined that the user computer contains the new antivirus file not contained within the central service computer" (see this or similar, but not identical, language in each of the foregoing claims). For substantially the same reasons as argued above, applicant respectfully asserts that neither the Hodges nor Van Huben references teach such specific claim language.

Furthermore, the Examiner has responded to applicant's arguments with respect to applicant's claimed technique "wherein the central service computer is configured to periodically obtain updated antivirus files from the antivirus server." Specifically, the Examiner has stated the "Hodges teaches notifying server of user update requirements

(CL9-L53-55,CL9-L62-67, Fig. 7), new virus definitions (CL5-41), antivirus signature files (CL8-L51-65, Fig. 5b), automatic (i.e. periodic) file updating (CL5-L29), and version number (CL9-L47, CL16-L27)." The Examiner has further referenced McAfee Orchestrator in relying on "programmable intelligent agents for reporting back any antivirus events to the server (pp. 16), and controlling antivirus file downloads and periodic updates (pp. 11-18)).

Applicant respectfully asserts that the excerpts relied on by the Examiner only teach an "antivirus server...[that] updates the subscriber database" and "an antivirus database...[with] latest available versions [of virus signature files and executable program files]." Clearly, such teachings relate to the antivirus server itself having the latest available virus signature files, and not to a "central service computer [that] is configured to periodically obtain updated antivirus files from the antivirus server," as claimed by applicant (emphasis added). Furthermore, applicant notes that McAfee Orchestrator, as relied on by the Examiner, only teaches updates for user computers (see specifically page 11, last paragraph), and not for a central service computer, in the specific context claimed by applicant.

In addition, the Examiner has responded to applicant's arguments with respect to applicant's claimed "notifying the central service computer of the new antivirus data file located on the user computer, and the user computer inquiring whether to update the antivirus database with new antivirus files... wherein after the central service computer is notified of the new antivirus data file located on the user computer, the user computer waits for a request from the central service computer to send the new antivirus data file." Specifically, the Examiner has stated that "Hodges teaches notifying [the] server of user requirements...and new virus definitions." The Examiner has further stated that "'[w]aiting' from the central computer before sending a new file would obviously be necessary for synchronization purposes." In making such arguments, the Examiner has also referenced pp. 11-18 in McAfee Orchestrator.

With respect to the Hodges reference, applicant respectfully asserts that simply notifying a server of user update requirements, as in Hodges, does not meet applicant's specific claim language, namely "notifying the central service computer of the new antivirus data file located on the user computer" (emphasis added). In addition, the "new virus definitions" relied on by the Examiner relate to "updates [for] user desktops" (see Col. 5, lines 41-43). Clearly, virus definitions for user computers does not meet applicant's claimed "user computer [that] waits for a request from the central service computer to send the new antivirus data file" (emphasis added). To emphasize, applicant claims that the user computer itself sends the new antivirus data file (see context of specific claim language highlighted above), and not merely virus definitions that are sent to user computers, as in Hodges.

With respect to the Examiner's argument that "waiting" would be obviously necessary, applicant respectfully disagrees. In particular, the Examiner has argued that "'[w]aiting' from the central computer before sending a new file would obviously be necessary for synchronization purposes" thus implying that the central computer is waiting to send the new file (emphasis added). Applicant, however, claims that "the user computer waits" (emphasis added), and not that the central computer waits, as the Examiner has argued. In addition, applicant claims that "the user computer waits for a request from the central service computer to send the new antivirus data file" (emphasis added), and not merely before sending a new file for synchronization purposes, as argued by the Examiner.

With respect to the Examiner's reliance on McAfee Orchestrator, applicant respectfully asserts that such reference only teaches updates for user computers (see page 11, last paragraph). Therefore, since McAfee Orchestrator only discloses new antivirus data files stored on a server for updating user computers (see page 11 specifically under the Server), such does not teach "notifying the central service computer of the new antivirus data file located on the user computer," as claimed by applicant (emphasis added).

Still yet, with respect to each of the independent claims, the Examiner has again argued, as in the Office Action dated 9/20/2005, that "McAfee Orchestrator realize[s] the claimed elements relating to notifying central service computer of new antivirus files, periodically obtaining antivirus files from the antivirus antivirus server, and waiting for request from central service computer for sending updates."

In making such arguments, it seems the Examiner has failed to consider the full context of applicant's claim language. For example, applicant claims "notifying the central service computer of the new antivirus data file located on the user computer" (emphasis added). As noted above, McAfee Orchestrator only teaches a server with updated data that provides updated data to user computers (see page 11 specifically), and therefore does not teach a "new antivirus data file located on the user computer" where the central service computer is notified of such data, in the context claimed by applicant (emphasis added).

In addition, applicant claims that "the central service computer is configured to periodically obtain updated antivirus files from the antivirus server" (emphasis added), and not merely that user computers are updated from the server as in McAfee Orchestrator (again, see page 11). Furthermore, applicant's claimed "user computer [that] waits for a request from the central service computer to send the new antivirus data file" is also not met by McAfee Orchestrator, since McAfee Orchestrator only teaches user computers that receive updates from a server, and not a user computer that waits for a request from a central service computer, in the context claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the

prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially included the subject matter of Claim 19 et al. into each of the independent claims.

With respect to the subject matter of Claim 19, presently incorporated into each of the independent claims, the Examiner has stated that applicant's claimed technique "wherein comparing the antivirus databases further comprises comparing the antivirus databases only if the new antivirus file was received from the antivirus server" is rendered obvious by the teachings of Van Huben relating to comparing databases between a central server and a client computer to facilitate updating (CL4-L29-32)." Applicant respectfully disagrees.

In particular, the excerpt relied on by the Examiner in Van Huben only generally discloses that "[d]uring replication, the data within a client computer's database is compared against the data on the host server and the computer with the oldest copy is updated with the most recent." Clearly, only generally disclosing synchronizing databases, as in Van Huben, does not even suggest "comparing the antivirus databases only if the new antivirus file was received from the antivirus server," as specifically claimed by applicant (emphasis added). Applicant notes that simply nowhere does Van Huben teach that any requirement be met in order to compare databases, let alone where such comparing is contingent upon "the new antivirus file [being] received from the antivirus server," as applicant claims.

In addition, to further distinguish the prior art of record, applicant has also incorporated the following highlighted claim language into each of the independent claims:

> "comparing the antivirus databases of the central service computer and the user computer if the new antivirus file was received at the central service computer from the antivirus server or if the new antivirus file was received at the user computer from the antivirus server, in order to determine if one of the databases contain a new antivirus file not contained within the other database;" and
>
> "wherein the user computer is configured to send the new antivirus file to the central service computer to update the virus database of the central service computer, if is determined that the user computer contains the new antivirus file not contained within the central service computer and if it is determined that the user computer is authorized to send new antivirus files to the central service computer to update the virus database"

Again, since at least the third element of the prima facie case of obviousness has not been met, as noted above, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 38-39 below, which are added for full consideration:

> "wherein after the user computer sends the new antivirus file to the central service computer to update the virus database of the central service computer, the central service computer sends the new antivirus file to other user computers located on the computer network to update the virus databases of the other user computers" (see Claim 38); and

"wherein the new antivirus file includes a set of fields comprising a date updated field referring to a last date the antivirus file was modified, a time field referring to a last time the antivirus file was modified, and a DAT version field referring to a latest version of a main antivirus data file that was used to scan a file for computer viruses" (see Claim 39).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P313/01.051.02).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100